

## **CLAIM AMENDMENTS**

### **Claim Amendment Summary**

#### **Claims pending**

- Before this Amendment: Claims 1-37.
- After this Amendment: Claims 1-37

**Non-Elected, Canceled, or Withdrawn claims:** none

**Amended claims:** 9

**New claims:** none

---

**Claims:**

**1. (Original)** A computer-readable medium having computer-executable instructions that, when executed by the system, performs a method comprising:

obtaining a message  $M$ ;

defining a vector  $v$  to be  $v_1, \dots, v_n$  based upon a predefined first hashing function of the message;

calculating a private key  $\alpha$  in accordance with this equation  
$$\alpha = \sum_{i=1}^n v_i \alpha_i \bmod m;$$

producing a signature  $S$  in accordance with this equation:  $S = \alpha H_2(M)$ ,  
where  $H_2(M)$  is a predefined second hashing function of the message;

indicating results based, at least in part, on the obtaining, defining, calculating, or producing.

**2. (Original)** A medium as recited in claim 1, wherein the results of the indicating comprises a message-and-signature pair  $(M, S)$ .

**3. (Original)** A medium as recited in claim 1, wherein the results of the indicating comprises a message-and-signature pair  $(M, \mu S)$  and the method further comprises calculating  $\mu = H_3(BK, M)$ , where BK is key and  $H_3(BK, M)$  maps  $M$  into an integer within a defined range.

**4. (Original)** A medium as recited in claim 1, wherein the  $\alpha_i$  are scaling factors for  $n$  discrete logs of  $\alpha_1 P, \dots, \alpha_n P$  base  $P$ , where  $n$  is a positive integer,  $P$  is a point on an elliptic curve and a public key.

**5. (Original)** A medium as recited in claim 1, wherein  $\alpha_i$  are scaling factors for  $n$  discrete logs of  $\alpha_1 P, \dots, \alpha_n P$  base  $P$ , where  $n$  is a positive integer, wherein  $P$  is a point on an elliptic curve; a point  $P$  is of order  $m$  and where  $e_m(P, Q): E[m] \times E[m] \rightarrow GF(q)^*$  denotes a Tate or Weil or Squared Tate or Squared Weil Pairing, where  $\alpha_1 P, \dots, \alpha_n P = Q_1, \dots, Q_n$  and where  $q$  is a prime power.

**6. (Original)** A medium as recited in claim 1, wherein the signature  $S$  is represented by a number of bits, wherein the method further comprises truncating a specific number of bits off of  $S$  before the indicating.

**7. (Original)** A medium as recited in claim 1, wherein the first hashing function produces values in  $\{\pm 1\}$ .

**8. (Original)** A computing device comprising:

an output device;

a medium as recited in claim 1.

**9. (Currently Amended)** A computer-readable medium having computer-executable instructions that, when executed by the system, performs a method comprising:

choosing  $n$  discrete logs of  $\alpha_1 P, \dots, \alpha_n P$  base  $P$ , where  $n$  is a positive integer,  $P$  is a point on an elliptic curve and a public key, and  $a_i$  is a scaling factor and a private key;

indicating results of the choosing;

forging one or more short digital ciphers based upon the indicated results of the choosing.

**10. (Original)** A medium as recited in claim 9, wherein a point  $P$  is of order  $m$  and where  $e_m(P, Q): E[m] \times E[m] \rightarrow GF(q)^*$  denotes a Tate or Weil or Squared Tate or Squared Weil Pairing, where  $\alpha_1 P, \dots, \alpha_n P = Q_1, \dots, Q_n$  and where  $q$  is a prime power.

**11. (Original)** A medium as recited in claim 9 further comprising generating a digital signature based upon a message  $M$  and  $a_i$ .

**12. (Original)** A computing device comprising:

an output device;

a medium as recited in claim 9.

**13. (Original)** A method facilitating the production of a digital signature, the method comprising:

obtaining a message  $M$ ;

defining a vector  $v$  to be  $v_1, \dots, v_n$  based upon a predefined first hashing function of the message;

calculating a private key  $a$  in accordance with this equation  
$$\alpha = \sum_{i=1}^n v_i \alpha_i \bmod m ;$$

producing a signature  $S$  in accordance with this equation:  $S = aH_2(M)$ , where  $H_2(M)$  is a predefined second hashing function of the message;

indicating results based, at least in part, on the obtaining, defining, calculating, or producing.

**14. (Original)** A method as recited in claim 13 wherein the results of the indicating comprises a message-and-signature pair  $(M, S)$ .

**15. (Original)** A method as recited in claim 13, wherein the results of the indicating comprises a message-and-signature pair  $(M, \mu S)$  and the method further comprises calculating  $\mu = H_3(BK, M)$ , where BK is key and  $H_3(BK, M)$  maps  $M$  into an integer within a defined range.

**16. (Original)** A method as recited in claim 13, wherein the  $\alpha_i$  are scaling factors for  $n$  discrete logs of  $\alpha_1 P, \dots, \alpha_n P$  base  $P$ , where  $n$  is a positive integer,  $P$  is a point on an elliptic curve and a public key.

**17. (Original)** A method as recited in claim 13, wherein  $\alpha_i$  are scaling factors for  $n$  discrete logs of  $\alpha_1 P, \dots, \alpha_n P$  base  $P$ , where  $n$  is a positive integer,  $P$  is a point on an elliptic curve;  
a point  $P$  is of order  $m$  and where  $e_m(P, Q): E[m] \times E[m] \rightarrow GF(q)^*$  denotes a Tate or Weil or Squared Tate or Squared Weil Pairing, where  $\alpha_1 P, \dots, \alpha_n P = Q_1, \dots, Q_n$  and where  $q$  is a prime power.

**18. (Original)** A method as recited in claim 13, wherein the signature  $S$  is represented by a number of bits, wherein the method further comprises truncating a specific number of bits off of  $S$  before the indicating.

**19. (Original)** A method as recited in claim 13, wherein the first hashing function produces values in  $\{\pm 1\}$ .

**20. (Original)** A computer-readable medium having computer-executable instructions that, when executed by the system, performs a method comprising:

obtaining an input message-and-signature pair  $(M, S)$ ;

defining a vector  $v$  to be  $v_1, \dots, v_n$  based upon a predefined first hashing function of the message;

calculating a point  $Q$  on an elliptic curve in accordance with this equation:

$$Q = \sum_{i=1}^n v_i Q_i;$$

comparing pairing outputs of a pair  $(P, S)$  and a pair  $(Q, H_2(M))$ , where  $H_2(M)$  is a predefined second hashing function of  $M$  and  $P$  is a point on the elliptic curve;

indicating results of the comparing.

**21. (Original)** A medium as recited in claim 20 further comprising verifying the input message-and-signature pair  $(M, S)$  when the indicated results of the comparing is a match.

**22. (Original)** A medium as recited in claim 20, wherein:

the point  $P$  being a point on an elliptic curve and of order  $m$  and where  $e_m(P, Q) : E[m] \times E[m] \rightarrow GF(q)^*$  denotes a Tate or Weil or Squared Tate or Squared Weil Pairing, where  $\alpha_1 P, \dots, \alpha_n P = Q_1, \dots, Q_n$  and where  $q$  is a prime power;

the  $\alpha_i$  being scaling factors for  $n$  discrete logs of  $\alpha_1 P, \dots, \alpha_n P$  base  $P$ , where  $n$  is a positive integer.

**23. (Original)** A medium as recited in claim 20, wherein the method further comprises, when the indicated results of the comparing is not a match, modifying the vector  $v$  relative to its previous definition and repeating the defining, calculating, and comparing.

**24. (Original)** A medium as recited in claim 20, wherein the method further comprises:

when the indicated results of the comparing is not indicate a match, modifying the vector  $v$  relative to its previous definition;

repeating the defining, calculating, and comparing;

if the indicated results of the comparing still does not a match, then repeating the modifying and the repeating of the defining, calculating, and comparing until the indicated results do match.

**25. (Original)** A medium as recited in claim 20, wherein the method further comprises when the indicated results of the comparing is not a match, repeating the defining, calculating, and comparing with the defining being based upon a predefined third hashing function of the message.

**26. (Original)** A medium as recited in claim 20, wherein the signature  $S$  is represented by a number of bits, wherein the method further comprises padding  $S$  with a specific number of bits before the defining.

**27. (Original)** A computing device comprising:

an output device;

a medium as recited in claim 20.

**28. (Original)** A method facilitating the verification of a digital signature, the method comprising:

obtaining an input message-and-signature pair  $(M, S)$ ;

defining a vector  $v$  to be  $v_1, \dots, v_n$  based upon a predefined first hashing function of the message;

calculating a point  $Q$  on an elliptic curve in accordance with this equation:

$$Q = \sum_{i=1}^n v_i Q_i;$$

comparing pairing outputs of a pair  $(P, S)$  and a pair  $(Q, H_2(M))$ , where  $H_2(M)$  is a predefined second hashing function of  $M$  and  $P$  is a point on the elliptic curve;

indicating results of the comparing.

**29. (Original)** A method as recited in claim 28 further comprising verifying the input message-and-signature pair  $(M, S)$  when the indicated results of the comparing is a match.

**30. (Original)** A method as recited in claim 28, wherein

the point  $P$  being a point on an elliptic curve and of order  $m$  and where  $e_m(P, Q) : E[m] \times E[m] \rightarrow GF(q)^*$  denotes a Tate or Weil or Squared Tate or Squared Weil Pairing, where  $\alpha_1 P, \dots, \alpha_n P = Q_1, \dots, Q_n$  and where  $q$  is a prime power;

the  $\alpha_i$  being scaling factors for  $n$  discrete logs of  $\alpha_1 P, \dots, \alpha_n P$  base  $P$ , where  $n$  is a positive integer.

**31. (Original)** A method as recited in claim 28 further comprising, when the indicated results of the comparing is not a match, modifying the vector  $v$  relative to its previous definition and repeating the defining, calculating, and comparing.

**32. (Original)** A method as recited in claim 28 further comprising:  
when the indicated results of the comparing is not a match, modifying the vector  $v$  relative to its previous definition;  
repeating the defining, calculating, and comparing;  
if the indicated results of the comparing still does not a match, then repeating the modifying and the repeating of the defining, calculating, and comparing until the indicated results do match.

**33. (Original)** A method as recited in claim 28 further comprising when the indicated results of the comparing is not a match, repeating the defining, calculating, and comparing with the defining being based upon a predefined third hashing function of the message.

**34. (Original)** A method as recited in claim 28, wherein the signature  $S$  is represented by a number of bits, wherein the method further comprises padding  $S$  with a specific number of bits before the defining.

**35. (Original)** A computer-readable medium having computer-executable instructions that, when executed by the system, performs a method comprising:

obtaining an input message-and-signature pair  $(M, S')$ ;

defining a vector  $v$  to be  $v_1, \dots, v_n$  based upon a predefined first hashing function of the message;

calculating a point  $Q$  on an elliptic curve in accordance with this equation:

$$Q = \sum_{i=1}^n v_i Q_i;$$

comparing pairing outputs of a pair  $(P, S')$  and a pair  $(Q, H_2(M))^\mu$ , where  $H_2(M)$  is a predefined second hashing function of  $M$  and  $P$  is a point on the elliptic curve and  $\mu$  is an integer in a defined range;

indicating results of the comparing.

**36. (Original)** A medium as recited in claim 35 further comprising verifying the input message-and-signature pair  $(M, S)$  when the indicated results of the comparing is a match.

**37. (Original)** A computing device comprising:  
an output device;  
a medium as recited in claim 35.